The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
08/07/2012

SUBJECT:
Multiple Denial of Service Vulnerabilities in Cisco Products

OVERVIEW:
Multiple vulnerabilities have been discovered in several Cisco products including Cisco Adaptive Security Appliance (ASA) 5500 series appliances, Cisco devices running Cisco IOS, NX-OS, or MDS NX-OS, as well as Cisco's Unified Computer System (UCS) and AnyConnect Secure Mobility Client.

Successful exploitation of these vulnerabilities could result in denial of service conditions or a reload on the affected device.

SYSTEMS AFFECTED:

- Cisco ASA 5500 Series Adaptive Security Appliances prior to 8.2.5
- Cisco IOS 12.0(33)S, Cisco IOS 12.2, Cisco IOS 12.2, Cisco IOS 12.3, Cisco IOS 12.4(15)T10, Cisco IOS 15.0 M, Cisco IOS 15.1, Cisco IOS 15.2
- Cisco NX-OS 4.2, Cisco NX-OS 5.0, Cisco NX-OS 5.1, Cisco NX-OS 5.2, Cisco NX-OS 5.2(1)
- Cisco Unified Computing System (UCS) 1.4, Cisco Unified Computing System (UCS) 2.0, Cisco Unified Computing System (UCS) 2.0(1M)
- Cisco AnyConnect Secure Mobility Client 3.0

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: NA

DESCRIPTION:
Multiple Cisco products are vulnerable to remote Denial of Service due to the improper handling of exceptions. The details of each vulnerable Cisco product are provided below.

Cisco Operating Systems
The Cisco operating systems affected by these vulnerabilities are Cisco IOS, NX-OS, and MDS NX-OS. Cisco IOS runs on a variety of Cisco networking devices, Cisco NS-OS runs on Cisco switches, and Cisco MDS NX-OS runs on Cisco MDS series switches.

To exploit these vulnerabilities, an attacker needs to create a specially crafted packet that, when processed, may result in the denial of service conditions. The details of the vulnerabilities are as follows:

- Improper handling of a specially crafted BGP UPDATE message with a crafted local-preference attribute lengthsent to a device running a vulnerable version of Cisco IOS can cause the device to crash, resulting in a denial-of-service condition. This issue is being tracked by Cisco bug ID CSCtq06538 (CVE-2012-1367).
- Improper handling of a specially crafted Cisco Discovery Protocol (CDP) packet sent to a Nexus 7000 series switch running a vulnerable version of Cisco NX-OS can cause the device to crash, resulting in a denial-of-service condition. This issue being tracked by Cisco bug ID CSCtk34535 (CVE-2012-2469).
- Improper handling of a specially crafted packet sent to a device running a vulnerable version of Cisco IOS configured with clientless SSL VPN may cause the SSL VPN portal page to refresh, crashing the device and resulting in a denial-of-service condition. This issue is being tracked by Cisco bug ID CSCtr86328 (CVE-2012-1344)
- Improper handling of a specially crafted IAPP (Inter-Access Point Protocol (802.11 wireless extension)) packet sent to a device running a vulnerable version of Cisco IOS can cause the device to crash, resulting in a denial-of-service condition. This issue being tracked by Cisco bug ID CSCtc12426 (CVE-2012-1350).
- Improper handling of a packet with a specially crafted Fiber Channel over IP (FCIP) header sent to a device running a vulnerable version of Cisco MDS NX-OS can cause the device to crash, resulting in a denial-of-service condition. Cisco bug ID CSCtn93151 (CVD-2012-1340) is tracking this issue.

Cisco ASA Products
Cisco ASA products provide firewall, intrusion prevention, remote access, and other services.

Cisco ASA 5500 series appliances are prone to remote Denial of Service vulnerabilities due to the improper handling of exceptions. To exploit the vulnerabilities, an attacker needs to create a specially crafted packet that, when processed, may result in a denial of service condition. The details of the vulnerabilities are as follows:

- Improper handling of a specially crafted packet sent to a device used for Voice over IP (VoIP) can cause many identical “pinholes” (Dynamic Ports) to be created when Session Initiation Protocol (SIP) Inspection is enabled. The multiple identical pinholes may allow excessive CPU consumption, resulting in a Denial of Service condition on the device. This issue is being tracked by Cisco bug ID CSCtz63143 (CVE-2012-2472).
- Improper handling of a specially crafted packet sent to a WebVPN configured device may allow an attacker to cause excessive memory consumption by the device, resulting in

a denial-of-service condition. This issue being tracked by Cisco bug ID CSCth34278 (CVE-2012-2474)

Cisco Unified Computer System (UCS)
The Cisco Unified Computing System (UCS) is an x86 architecture data center server platform composed of computing hardware, virtualization support, switching fabric, and management software.

To exploit the vulnerabilities in the Cisco UCS, an attacker needs to create a specially crafted packet that, when processed, may result in the denial of service conditions. The details of the vulnerabilities are as follows:

- Improper handling of a specially crafted SNMP (Simple Network Management Protocol) request sent to a Fabric Interconnect device running a vulnerable version of Cisco UCS can cause the device to reload, resulting in a denial-of-service condition. This issue being tracked by Cisco bug IDs CSCts32452 and CSCts32463 (CVE-2012-1364 and CVE-2012-1365).
- Improper handling of a specially crafted request sent over SSH to a Fabric Interconnect device running a vulnerable version of Cisco UCS cause the SSHD process to crash, resulting in a denial-of-service condition. Cisco bug ID CSCtt94543 (CVE-2012-1339) is tracking this issue.

Cisco AnyConnect Secure Mobility Client
Cisco AnyConnect Secure Mobility Client is a VPN client application that provides secure remote connections to specific Cisco devices.

To exploit the vulnerability in Cisco AnyConnect Secure Mobility Client, an attacker needs to create a specially crafted packet that, when processed, may result in the denial of service conditions. The details of the vulnerability is as follows:

- Improper handling of a specially crafted packet sent to a vulnerable version of Cisco AnyConnect client can cause the 'vpnagentd' service, and subsequently the application, to crash, resulting in a denial-of-service condition. This issue being tracked by Cisco bug ID CSCty01670 (CVE-2012-1370).

RECOMMENDATIONS:
The following actions should be taken:

- Upgrade vulnerable Cisco products immediately after appropriate testing.

REFERENCES:

Cisco:
http://www.cisco.com/en/US/docs/security/asa/asa84/release/notes/asarn84.html
http://www.cisco.com/web/software/280775065/45357/ASA-825-Interim-Release-Notes.html
http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_category_home.html
http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/release/notes/52_nx-os_release_note.html
http://www.cisco.com/en/US/docs/ios/15_1/release/notes/151-2TCAVS.html
http://www.cisco.com/en/US/docs/wireless/access_point/ios/release/notes/12_3_8_JED1rn.html
http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/sw/5_2/release/notes/nx-os/mds_nxos_rel_notes_522.html
http://www.cisco.com/en/US/docs/unified_computing/ucs/release/notes/OL_24086.html
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/release/notes/anyconnect30rn.html
http://www.cisco.com/en/US/docs/unified_computing/ucs/release/notes/OL_25363.html

SecurityFocus:
http://www.securityfocus.com/bid/54836
http://www.securityfocus.com/bid/54840
http://www.securityfocus.com/bid/54830
http://www.securityfocus.com/bid/54833
http://www.securityfocus.com/bid/54835
http://www.securityfocus.com/bid/54837
http://www.securityfocus.com/bid/54843
http://www.securityfocus.com/bid/54829
http://www.securityfocus.com/bid/54841
http://www.securityfocus.com/bid/54842

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2472
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2474
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1367
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2469
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1344
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1350
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1340
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1364
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1365
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1370
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1339